VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Monitorování parametrů v mobilních sítích druhé generace pomocí PDA.

Monitoring of Parameters in Second Generation of Mobile Networks for PDA

2010 Bc. Martin Raichl

Souhlasím se zveřejněním této diplomové práce dle požadavků čl. 26, odst. 9 *Studijního a zkušebního řádu pro studium v magisterských programech VŠB-TU Ostrava*.

V Ostravě 7. května 2010 .....

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 7. května 2010 .....

Na tomto místě bych rád poděkoval rodině za podporu při studiu a vedoucímu diplomové práce Ing. Liboru Michálkovi, Ph.D., který mi poskytl odbornou pomoc při zpracování této diplomové práce.

Abstrakt

Cílem práce je analyzovat rozhraní PDA pro komunikaci s GSM modulem a následné vytvoření aplikace pro sledování identifikátorů v sítích GSM 2. generace. Součástí práce je také testování aplikace v reálných podmínkách, na zařízeních různých výrobců.

K aplikaci je zpracována uživatelská a programátorská dokumentace.

Klíčová slova: GSMinfo, identifikátory GSM 2. generace, RIL

Abstract

The aim of the thesis is to analyze PDA interface for communication with a GSM module and the creation of application for tracking of identifiers in GSM networks 2nd generation. The thesis also includes testing of applications under real conditions on the devices of different brands.

Manual for users and programmers is processed for the application.

Keywords: GSMinfo, identifiers in GSM networks 2nd generation, RIL

Seznam použitých zkratek a symbolů

Zkratka	-	**Význam zkratky**	-	**Český význam zkratky**
A	-			
AGCH	-	Access Grant Channel	-	potvrzovací kanál
AMPS	-	Advanced Mobile Phone Service	-	systém pro mobilní komunikaci
API	-	Application Programming Interface	-	aplikační programové rozhraní
ARFCN	-	Absolute Radio Frequency Channel Number	-	číslo rádiového kanálu
ARM	-	Advanced RISC Machine	-	pokročilé RISC stroje
AUC	-	Authentication Center	-	autentizační centrum
B	-			
BCC	-	Base Transceiver Station Color Code	-	kód základnové stanice
BCCH	-	Broadcast Control Channel	-	vysílací řídící kanál
BER	-	Bit Error Ratio	-	bitová chybovost
BTS	-	Base Tanceiver Station	-	základnová stanice
BSC	-	Base Station Controller	-	základnová řídící jednotka
C	-			
CC	-	Country Code	-	kód země
CCCH	-	Common Conttrol Channel	-	běžný řídící kanál
CBCH	-	Cell Broadcast Channel	-	vysílací kanál buňky
CDMA	-	Code Division Multiple Access	-	mnohonásobný kódový přístup
CI	-	Cell Identifier	-	identifikátor buňky

CLI	-	Common Language Infrastructure	-	společná infrastruktura programovacích jazyků
CLR	-	Common Language Runtime	-	mechanismus zodpovědný za spuštění kódu
D	-			
D-AMPS	-	Digital-Advanced Mobile Phone Service	-	digitální systém pro mobilní komunikaci
DCCH	-	Dedicated Control Channel	-	dedikovaný řídící kanál
DCS 1800	-	Digital Cellular System	-	digitální celulární systém
E	-			
EDGE	-	Enhanced Data For GSM Evolution	-	vývojový stupeň v technologii GSM po zavedení datových přenosů pomocí GPRS
EGSM	-	Extended GSM	-	rozšířený GSM systém
EIR	-	Equipment Identity Register	-	registr mobilních stanic
ExTAPI	-	Extended API	-	rozšířené API
F	-			
FAC	-	Final Assembly Code	-	závěrečný montážní kód
FACCH	-	Fast Associated Control Channel	-	rychlý přidružený řídící kanál
FCCH	-	Frequency Correction Channel	-	frekvenčně korekční kanál
FDD	-	Frequency Division Duplex	-	kmitočtově dělený duplex
FDMA	-	Frequency Division Multiple Access	-	kmitočtově dělený mnohonásobný přístup
G	-			
GPS	-	Global Position System	-	globální systém určování geografické polohy
GPRS	-	General Packet Radio Services	-	paketově orientovaná datová služba

GUI	-	Graphic User Interface	-	grafické uživatelské rozhraní
H	-			
HLR	-	Home Location Register	-	domovský lokační registr
I	-			
IMEI	-	International Mobile Station Equipment Identity	-	unikátní číslo mobilního zařízení
IMSI	-	International Mobile Subscriber Identification	-	unikátní zákaznické identifikační číslo
L	-			
LAC	-	Location Area Code	-	kód oblasti
LMSI	-	Local Mobile Station Identity	-	lokální identita mobilní stanice
LMT	-	Local Maintance Terminal	-	místní údržbový terminál
M	-			
MAHO	-	Mobile Assisted Handover	-	sítí řízený handover s asistencí mobilní stanice
MCC	-	Mobile Country Code	-	kód země
MCHO	-	Mobile Controlled Handover	-	handover řízený mobilní stanicí
MDA	-	Mobile Device Assistent	-	mobilní komunikační zařízení
MIPS	-	Microprocessor without Interlocked Pipeline Stages	-	procesor bez automaticky organizované pipeline
MNC	-	Mobile Network Code	-	kód mobilní sítě
MS	-	Mobile Station	-	mobilní stanice
MSC	-	Mobile Switching Center	-	radiotelefonní ústředna
MSIN	-	Mobile Subscriber Identification Number	-	kód mobilního účastníka v rámci sítě operátora
MSISDN	-	Mobile Subscriber ISDN Number	-	mobilní telefonní číslo účastníka
N	-			

NCC	-	Network Color Code	-	kód sítě
NDC	-	National Destination Code	-	národní směrové číslo
NCH	-	Notification Channel	-	oznamovací kanál
NCHO	-	Network Controlled Handover	-	sítí řízený handover
NMT	-	Nordic Mobile Telephone	-	standard pro mobilní telefony
NSS	-	Network Switching System	-	síťový přepínací subsystém
O	-			
OSS	-	Operation Support Subsystem	-	operační a podpůrný subsystém
P	-			
PGSM	-	Primary GSM	-	primární GSM
PCH	-	Paging Channel	-	kanál pro paging
R	-			
RACH	-	Random Access Channel	-	kanál náhodného přístupu
S	-			
SACCH	-	Slow Associated Control Channel	-	pomalý přidružený řídící kanál
SDK	-	Software Development Kit	-	balík pro vývoj softwaru
SCH	-	Synchronization Channel	-	synchronizační kanál
SDCCH	-	Standalone Dedicated Control CHannel	-	samostatný přidělený řídící kanál
SIM	-	Subscriber Identity Module	-	účastnický identifikační modul
SMSCB	-	Short Message Service Cell Broadcast	-	vysílání zpráv služby krátkých textových zpráv buňky
SNR	-	Serial Number	-	sériové číslo
SN	-	Subscriber Number	-	číslo účastníka
T	-			
TAC	-	Type Approval Code	-	kód typu homologace
TACS	-	Total Access Control System	-	upravený systém AMPS

TAPI	-	Telephony Application Programming Interface	-	programátorské rozhraní zaměřené na telefonii
TDMA	-	Time Division Multiple Access	-	časově dělený mnohonásobný přístup
TCH	-	Traffic Channels	-	provozní kanály
TMSI	-	Temporaly Mobile Subscriber Identity	-	dočasná účastnická identita
TRAU	-	Tanscoder and Rate Adaptor Unit	-	transkódovací jednotka
TS	-	Time Slot	-	časový slot
U	-			
UML	-	Unified Modeling Language	-	grafický jazyk pro objektově orientovanou analýzu a návrh softwaru
UMTS	-	Universal Mobile Telecominication System	-	systém 3. generace standardu mobilních telefonů
V	-			
VLR	-	Visitor Location Register	-	návštěvnický lokační registr
W	-			
WCF	-	Windows Communication Foundation	-	základní infrastruktura sjednocující starší technologie korporace Microsoft
WiFi	-	Wireless Fidelity	-	standard pro lokální bezdrátové sítě
WiMAX	-	Worldwide Interoperability for Microwave Access	-	technologie pro širokopásmový bezdrátový přístup
WM	-	Windows Mobile	-	operační systém pro mobilní zařízení

Obsah

Seznam tabulek

Seznam obrázků

Seznam výpisů zdrojového kódu

1 Úvod

Systém GSM patří do druhé generace radiotelefonních systémů, které jsou plně digitální a jsou připraveny poskytnout vyšší kvalitu spojení, služeb i zabezpečení. Tento systém byl od počátku vyvíjen pro hlasovou komunikaci uživatelů po celém světě. Postupem času nabídl datové a multimediální služby v podobě různých rozšíření. Skrytý potenciál tohoto systému tkví v jeho architektuře v podobě informací, které jsou využívány pro řízení systému a jsou běžným uživatelům skryty, v podobě nic neříkajících čísel či znacích, v nižších vrstvách telefonního přístroje. Některé telefonní přístroje na různých platformách nabízejí servisní menu, které dokáže zpřístupnit identifikátory sítě. Tyto přístroje jsou vyhledávány (ve většině případů) servisními techniky systému GSM nebo nadšenci, zajímajícími se hlouběji o problematiku GSM. Dnešní rychle se rozvíjející trend posunul komunikační zařízení na velmi vysokou úroveň. Této úrovně bylo dosaženo především využitím pokročilých operačních systémů v mobilních zařízení komunikujících v síti GSM. Operační systém je daleko flexibilnější a nabízí mnohá rozšíření oproti „hloupým“ softwarům, kterými byly vybavovány standardně mobilní přístroje. Dnes se mezi nejpoužívanější operační systémy řadí systém Windows Mobile od společnosti Microsoft. Z tohoto předpokladu vychází i zadání této diplomové práce. Tedy vyvinout servisní menu, které umožní zobrazit jinak skryté identifikátory sítě GSM 2. generace na zařízeních se systémem Windows Mobile a platformou .NET.

V úvodních kapitolách nastíním problematiku GSM systému se zaměřením na zmíněné identifikátory sítě. V následujících kapitolách objasním problematiku týkající se mobilních zařízení s operačním systémem Windows Mobile a jejich komunikaci s integrovaným GSM modulem. Po patřičné analýze a návrhu implementuji řešení v podobě aplikace, která prostřednictvím modemu v zařízení zobrazí obsluze požadované identifikátory sítě. Finální řešení podrobím testování v reálných podmínkách a v samotném závěru zhodnotím využití mobilních zařízení s OS Windows Mobile v této oblasti. V závěru se pokusím také nastínit již výše zmíněný potenciál spočívající ve znalosti identifikátorů sítě.

2 Radiotelefonní systémy

Radiotelefonní systémy jsou bezdrátovou obdobou pevných telekomunikačních sítí s velkou výhodou, kterou je mobilita účastníka. Radiotelefonní systémy umožňují uživatelům využívat telekomunikační služby kdekoliv, bez závislosti na pevných přípojkách.

2.1 Generace radiotelefonních systémů

- *1. generace* - analogové systémy zaměřené primárně na přenos hlasu, data pouze v omezené míře. Systémy využívají techniku frekvenčně děleného multiplexu FDMA (Frequency Division Multiple Access). Pro jednotlivé hovory se používají vždy celé frekvenční kanály. Mezi tyto systémy se řadí např. AMPS (Advanced Mobile Phone Service) v USA, NMT (Nordic Mobile Telephone) v Evropě a upravený systém TACS (Total Access Control System) vycházející z AMPS, používaný ve Velké Británii.

- *2. generace* - označuje digitální systémy využívající techniku přístupu časového multiplexu TDMA (Time Division Multiple Access). Metoda TDMA efektivně přiřazuje účastníkovi část frekvenčního spektra. Do této generace spadají digitální systémy GSM 900, DCS 1800 (Digital Cellular System), D-AMPS (Digital-Advanced Mobile Phone Service) PDC 1900 (Personal Digital Cellular), Digital TDM a další. Tyto systémy se orientují na poskytování hlasových služeb, ale s dalším rozvojem se objevují i doplňující nehlasové služby, poskytované koncovým uživatelům.

- *2,5 a 2,75 generace* - tyto generace rozšiřují stávající systémy druhé generace o paketový přenos dat změnou modulace na rádiovém rozhraní. Paketový přenos dat v 2,5 generaci zajišťuje technologie GPRS (General Packet Radio Services), která je doplněním mobilní sítě. EDGE (Enhanced Data For GSM Evolution) je dalším rozšířením systému GSM o vysokorychlostní přenos dat a služeb s tím spojených. EDGE se řadí do generace 2,75.

- *3. generace* - třetí generace je primárně vyvíjena pro vysokorychlostní přenos dat. Přenos dat zajišťuje digitální systém v Evropě nazvaný UMTS (Universal Mobile

Telecominication System), v Americe označený jako CDMA 2000 (Code Division Multiple Access).

- *4. generace* - jsou sítě pracující na internetové technologii a kombinují se s technologiemi jako WiFi, WiMAX apod. Přenosové rychlosti se pohybují v desítkách Mbit/s v buňkově strukturovaných sítí a ve stovkách Mbit/s v lokálních např. WiFi sítích.

3 GSM systém

Globální systém pro mobilní komunikaci (GSM - Global system for mobile communication) je celosvětově uznávaný standard pro celulární digitální mobilní komunikace druhé generace. GSM je název skupiny standardizace založené v roce 1982 k vytvoření společného evropského standardu mobilních telefonů, který formuluje požadavky mobilních rádiových operačních systémů na 900 MHz. GSM díky plné digitalizaci poskytuje širší nabídku služeb a umožňuje kompatibilitu s jinými digitálními sítěmi po celém světě - roaming.

- *GSM 450* - mobilní komunikace využívá pásmo 450 MHz již od osmdesátých let analogovou technologií NMT (Nordic Mobile Telephone). Tyto analogové sítě nemají žádnou budoucnost v pokrokových zemích, proto se toto pásmo digitalizovalo a někteří mobilní operátoři v tomto pásmu poskytují datové služby např. CDMA 450.

- *PGSM (Primary GSM)* - primární systém GSM, též označovaný jako GSM 900. Systém operuje v kmitočtovém pásmu od 890 MHz do 960 MHz, rozděleného do dvou částí. 890 - 915 MHz pro směr od MS (Mobile Station) k BTS (Base Tanceiver Station), (tzv. uplink) a 935 - 960 MHz pro směr od BTS k MS (tzv. downlink). Jako přístupovou techniku se zde využívá FDMA a kmitočtový duplex FDD (Frequency Division Duplex). Základnové stanice (BTS) vysílají na vyšším kmitočtu duplexního páru o šířce 45MHz. Každé pásmo obsahuje 124 rádiových kanálů a každý tento kanál má šířku 200 kHz. Zbylá 200 kHz část pásma vytváří 2 x 100 kHz oddělovací úseky každého pásma na horním a spodním kraji pásma. Čísla jednotlivých kanálů označuje ARFCN (Absolute Radio Frequency Channel Number) hodnotami 1 až 124. V každém rádiovém kanálu vytváří metoda TDMA 8 časových intervalů, označovaných jako TS (Time Slot), které tvoří rámec (TDMA frame). Celkový počet duplexních účastnických kanálů je tedy 124 x 8 = 992.

- *EGSM (Extended GSM)* - rozšířený systém GSM - zde jsou kmitočtová pásma rozšířena na spodních okrajích o 10 MHz. Přidělené pásmo je tedy 880 - 960 MHz, rozdělené

na 880 - 915 MHz pro uplink a 925 - 960 MHz je pro downlink. Tím se zvýšil počet duplexních kanálů o 50. Celkový počet kanálů pro každé pásmo je 124.

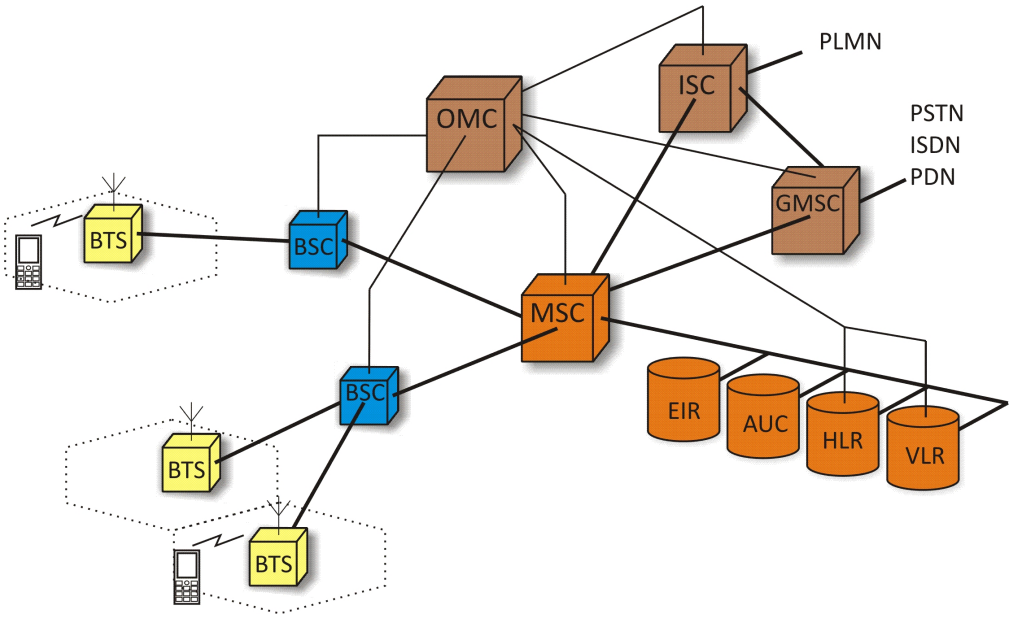
- *DCS-1800 (Digital Cellular System 1800) - systém GSM 1800* - využívá kmitočtové pásmo 1710 až 1880 MHz, rozdělené na 1770 - 1785 MHz pro uplink a 1805 - 1880 MHz pro downlink. Pásma obsahují 374 rádiových kanálů s odstupem 200 kHz, což dává dohromady 2992 rádiových kanálů. Systém má opět 100 kHz oddělovací úseky na spodních a horních okrajích každého pásma [1].

3.1 Architektura

Systém je postaven na buňkové (celulární) struktuře. Přínos této struktury sítě spočívá ve zmenšení plochy oblastí, které jsou obsluhovány určitými rádiovými kmitočty a relativně malým vysílacím výkonem vysílače. To umožňuje znovu využít stejný kmitočet u další buňky při minimálním rušení v blízkých oblastech. Velké území je tak rozděleno na několik menších oblastí (buněk). Tato koncepce umožňuje, z hlediska pokrytí území, téměř neomezenou kapacitu sítě. Uvnitř každé buňky je umístěna základnová rádiová stanice BTS (Basic Transceiver Station), která zprostředkovává spojení koncových uživatelů se systémem. Velikost buněk se stanoví dle kritérií, jako je předpokládané vytížení buňky a terénu, kde bude nasazena.

- *Makrobuňky* - mají poloměr desítky kilometrů. Jejich nasazení se týká rozsáhlých oblastí s malým provozem, jako jsou např. vesnice.
- *Mikrobuňky* - poloměr stovky metrů. Využití na území s velkým provozem typickým pro velká města.
- *Pikobuňky* - poloměr v desítkách metrů s využitím uvnitř budov.
- *Selektivní buňky* - jsou buňkami se směrovým vyzařováním.
- *Deštníkové (překrývající) buňky* - jsou větší buňky překrývající několik menších. Při rychlém pohybu v mikrobuňkové struktuře jsou předáni uživatelé těmto buňkám, které překrývají mezery mezi buňkami.

Několik buněk tvoří svazek. Činnost svazku řídí základnová řídící jednotka BSC (Base Station Controller). GSM síť se skládá z několika funkčních subjektů, které mají specifikované funkce a rozhraní. Obrázek 3.1 zobrazuje strukturu rozložení systému GSM. Systém GSM můžeme rozdělit do tří hlavních subsystémů - síťový přepínací subsystém, subsystém základnových stanic a operační a podpůrný subsystém.



Obrázek 3.1: Architektura systému GSM

3.1.1 Síťový přepínací subsystém NSS

Síťový přepínací systém NSS (Network Switching System) je zodpovědný za zpracování komunikace a další účastnické funkce mezi účastníky mobilní sítě GSM a externích telekomunikačních sítí. Spínací systém zahrnuje následující funkční celky:

- *Radiotelefonní ústředna MSC (Mobile Switching Center)* - tvoří spínací prvek v síti. To zahrnuje vyhledání cesty v síti k účastníkovi, směrování hovorů mezi BSC a jinými MSC, směrování datových provozů, výstavbu spojení, předávání účastníků mezi jednotlivými buňkami.

- *Domovský lokační registr HLR (Home Location Register)* - HLR má záznam pro všechny registrované účastníky operátora sítě. Uchovává informace o uživateli. Kromě fixních administračních údajů uchovává i dočasné údaje, například aktuální umístění účastníka.

- *Návštěvnický lokační registr VLR (Visitor Location Register)* - registr uchovávající informace o dočasných účastnících v „cizí“ síti.

- *Autentizační centrum AUC (Authentication Center)* - jednotka pro bezpečné ověření účastníků sítě, kteří jsou registrováni v HLR a VLR pomocí klíčů a bezpečnostních algoritmů.

- *Registr mobilních stanic EIR (Equipment Identity Register)* - registr obsahuje tzv. „černou“ listinu. Registr identifikuje neoprávněně užívané mobilní stanice na základě dat ověřovaných z HLR a VLR.

3.1.2 Subsystém základnových stanic BSS

BSS (Base Station System) - systém zajišťující přenos rádiových signálů (rádiový subsystém). Sestává se z následujících částí:

- *Základnové stanice BTS (Base Transceiver Station)* - obsluhuje rádiové rozhraní pro mobilní stanice. BTS je rádiové zařízení (vysílače, antény) potřebné k provozu každé buňky. Skupiny BTS jsou ovládány základnovou řídící jednotkou BSC.

- *Základnová řídící jednotka BSC (Base Station Controller)* - poskytuje funkce kontroly a fyzické spojení mezi MSC a BTS. Jedná se o vysoce kapacitní přepínač, který poskytuje funkce jako je handover, konfiguraci datových buněk, ovládání rádiových kmitočtů a výkonnostních úrovní BTS.

- *Transkódovací jednotka TRAU (Tanscoder and Rate Adaptor Unit)* - jednotka přizpůsobuje přenosové rychlosti dat. TRAU provádí také konverzi formátů použitých kodeků hlasu.

- *Místní údržbový terminál LMT (Local Maintance Terminal)* - terminál sloužící pro údržbu a aktivaci základnové stanice.

3.1.3 Operační a podpůrný subsystém OSS

Operační a podpůrný subsystém OSS (Operation Support Subsystem) zajišťuje provoz celého systému. Techničtí pracovníci pomocí tohoto systému monitorují a diagnostikují, popřípadě opravují chyby v systému. Zajišťuje také registrace účastníků, jejich tarifování, diagnostikuje stanice a další funkce[4].

3.1.4 Mobilní stanice MS

Mobilní stanice MS (anglicky Mobile Station) je koncové zařízení na straně uživatele využívající služby v systému GSM. MS se skládá ze dvou základních částí. První častí je mobilní zařízení samo o sobě jako hardwarové řešení, které se sestává z několika funkčních bloků (řídící mikroprocesory, obvody pro zpracování signálů, vysokofrekvenční blok, ovládací prvky). Každé mobilní zařízení je jednoznačně identifikováno v síti pomocí svého unikátního čísla IMEI (International Mobile Equipment Identity) uloženého v interní paměti. Mobilní stanice obsluhuje zabezpečení, kódování, šifrování, přenos hovorových a datových signálů. Monitoruje kvalitu a výkon signálu na aktuálně připojené buňce a buňkách sousedních. Na základě těchto informací je prováděn handover. Důležitou druhou součástí MS je účastnický identifikační modul SIM.

3.1.5 SIM karta

SIM (Subscriber Identity Module) je ve formě čipové karty uvnitř mobilního zařízení. Identifikační modul obsahuje pamětí RAM, ROM a mikropočítač, který provádí operace nad daty v modulu uloženými. SIM identifikuje účastníka v síti na základě čísla IMSI (International Mobile Subscriber Identification), které je obsaženo v její paměti. Dále se v paměti SIM nachází účastnický ověřovací klíč K_i. Klíč zabezpečuje šifrování dat a ověřování oprávnění používaní služeb. Tento klíč je specifický pro každý modul. Druhým

klíčem v SIM je šifrovací klíč K_c. K_c je specifický dočasný klíč, generovaný na základě algoritmu A8 a klíče K_i. Klíč slouží ke spojení a šifrování přenášených dat.

3.2 Identifikace

Jako v každé komunikační síti musí být subjekty v síti GSM jednoznačně identifikovatelné. Nejznámějším identifikátorem v GSM je telefonní číslo uživatele. Kromě tohoto čísla je zapotřebí ještě několik identifikátorů, které jsou potřebné ke správě mobility uživatele a pro identifikaci všech zbývajících síťových prvků. V GSM se rozlišuje uživatel a jeho hardwarové vybavení zvlášť. Proto existují specifické identifikátory pro uživatele a identifikátory pro mobilní stanice. Uživatelské identity jsou uložené na kartě SIM, identity mobilních stanic jsou uloženy v zařízeních. Kromě tohoto rozlišení, GSM rozlišuje identitu uživatele a jeho telefonní číslo. To ponechává jistý prostor pro rozvoj služeb, nezávisle na dosažitelnosti nebo typu připojení (mobilní nebo pevné). V následující části jsou popsány nejdůležitější identifikátory používané v GSM.

3.2.1 Mezinárodní identita mobilních stanic IMEI

Patnácti-místné číslo IMEI (International Mobile Station Equipment Identity) jednoznačně identifikuje mobilní zařízení. Jedná se o druh sériového čísla přidělovaného výrobcem, které dává indicie o výrobci a datumu výroby zařízení. Identifikátor IMEI je registrován u operátora sítě, který jej uchovává v registru EIR za účelem identifikace například poškozených nebo odcizených zařízení. Pro tyto účely jsou operátory vytvářeny tři seznamy.

- Na takzvaném *"bílém seznamu"* jsou uvedeny IMEI všech zařízení v síti.
- *"Černý seznam"* obsahuje identifikátory stanic, které mají zakázanou registraci do sítě. Tento seznam je vyměňován mezi operátory sítí.
- Třetím volitelným seznamem je *"šedý seznam"*nesoucí identity zařízení, které mají zastaralé verze softwaru nebo mají poruchu. Taková zařízení mají přístup do sítě, ale jejich použití je hlášeno obsluhujícímu personálu.

IMEI se vyžaduje při registraci do sítě, ovšem je možné si ho vyžádat i opakovaně poté. IMEI je hierarchický identifikátor obsahující následující části.

- *Kód typu homologace TAC (Type Approval Code)* - šest číslic, kde první dvě nesou kód země.
- *Závěrečný montážní kód FAC (Final Assembly Code)* - dvě číslice (kód výrobce).
- *Sériové číslo telefonu SNR (Serial Number*) - šest číslic.
- *Číslo SP (Spare)* - náhradní (jedna) číslice, většinou nula.

3.2.2 Mezinárodní identita mobilního účastníka IMSI

Číslo IMSI (International Mobile Subscriber Identity) je přiřazováno operátorem novému účastníkovi, který se registruje do služeb sítě operátora. Tento jedinečný identifikátor je uložen na kartě SIM a je obsažen z patnáctimístného decimálního čísla složeného ze tří částí.

- *Kód země MCC (Mobile Country Code).*
- *Kód mobilního operátora MNC (Mobile Network Code).*
- Desetimístní kód mobilního účastníka v rámci sítě operátora *MSIN (Mobile Subscriber Identification Number)*, kde první dvojčíslí udává číslo HLR.

3.2.3 Mobilní účastnické číslo ISDN

Telefonní číslo na mobilní uživatele je nazýváno MSISDN (Mobile Subscriber ISDN Number). Toto číslo je přiděleno k účastníkovi resp. k jeho kartě SIM. K jedné SIM může být vázáno několik MSISDN čísel. S touto koncepcí byl GSM prvním mobilním systémem, který rozlišoval mezi účastnickou identitou (IMSI) a telefonním číslem (MSISDN). Oddělení identity a telefonního čísla účastníka slouží především k ochraně důvěrnosti IMSI. Na rozdíl od MSISDN nemusí být tedy IMSI nikde zveřejněno, to přispívá k lepší

ochraně proti podvržení identity účastníka. Mobilní účastnická čísla se řídí mezinárodním číslovacím plánem ISDN. Mají následující strukturu:

- *kód země CC (Country Code)* - jedno až tři čísla (pro ČR 420),
- *národní směrové číslo NDC (National Destination Code)* - dvě až tří číslice, identifikuje síť v příslušné zemi,
- *účastnické číslo SN (Subscriber Number)* - definuje konkrétní SIM v příslušné síti operátora, mohou mít proměnnou délku.

MSISDN jsou uložena centrálně v HLR.

3.2.4 Roamingové mobilní číslo stanice MSRN

MSRN (Mobile Station Roaming Number) je dočasné polohově závislé ISDN číslo, které přiděluje příslušný VLR ve své oblasti ve státě. K účastníkovi v roamingové oblasti jsou hovory směrovány právě na základě MSRN. Na požadavek je MSRN předáno z domovského HLR na GMSC. MSRN má stejnou strukturu jako MSISDN:

- *CC* navštívené země
- *NDC* navštívené země
- *SN* v domácí síti

3.2.5 Identifikátor oblasti LAI

Každá oblast celulární sítě má svůj vlastní identifikátor - LAI (Location area identity). LAI je hierarchicky strukturovaný a mezinárodně unikátní. Identifikátor se opět skládá z mezinárodně standardizované části a z části závislé na operátorovi.

- *CC*, tři číslice
- *MNC*, dvě číslice

- *LAC (Location Area Code)*, maximálně pět číslic nebo 2 x 8 bitů kódovaných v hexadecimální soustavě.

Tento LAI je vysílán pravidelně základnovou stanicí pomocí vysílacího řídícího kanálu BCCH (Broadcast Control Channel). Buňka je tedy jednoznačně identifikovatelná jako i její náležitost do oblasti. MS tedy může určit svoji aktuální polohu na základě LAI. Pokud MS zjistí změnu LAI, oznámí tuto skutečnost síti a požádá o aktualizaci informací v VLR a HLR. MS se podílí větší mírou o monitorování signálu v dané lokalitě a vybírá základnové stanice, které poskytují lepší signál. Po vhodném výběru základnové stanice se zapíše do VLR té oblasti do které základnová stanice patří. LAI je požadováno z VLR, pokud je příchozí volání směrováno k současnému MSC za použití MSRN. To určí přesné umístění MS.

3.2.6 Dočasná účastnická identita TMSI

VLR zodpovědný za informaci o aktuálním umístění účastníka může přiřadit účastníkovi dočasnou identitu TMSI (Temporaly Mobile Subscriber Identity), která má pouze lokální význam v oblasti, kterou daný VLR obsluhuje. To je použito na místo IMSI pro definitivní identifikaci a adresaci MS. Tímto způsobem je zamezena možnost zjištění totožnosti účastníka, případným poslechem rádiového kanálu. TMSI je přiděleno po dobu přítomnosti MS v oblasti jednoho VLR a může být měněno i po tuto dobu (ID hopping). MS ukládají TMSI na kartu SIM. Na straně sítě je TMSI uloženo pouze v VLR (nepředává se do HLR). Skládá se až ze 4 x 8 bitů v hexadecimální soustavě. Použitím LAI a TMSI společně může být účastník v síti jednoznačně identifikován, to znamená že IMSI může být nahrazeno touto dvojicí.

3.2.7 Ostatní identifikátory

VLR je schopno přiřadit další vyhledávací indexy mobilní stanici na svém území s cílem urychlit vyhledávání v databázi. Lokální identita mobilní stanice LMSI (Local Mobile Station Identity) je přiřazena, pokud se MS registruje ve VLR a registrace je také zasílána do HLR. LMSI již není v HLR využívané, ale pokud jsou zprávy týkající

se MS odesílány do VLR, je přidáno LMSI. Tento přidaný identifikátor zkracuje dobu hledání klíče pro operace týkající se dané MS. Tento druh identifikace je používaný pouze tehdy, kdy MSRN je nově přiřazeno s voláním. V tomto případě má rychlost zpracování důležitou váhu, pro dosažení krátké doby potřebné pro sestavení hovoru. Stejně jako TMSI je LMSI unikátní jen v rámci území spravovaného daným VLR. LMSI se skládá ze čtyř oktetů (4 x 8 bitů). Uvnitř oblasti jsou jednotlivé buňky jednoznačně označeny identifikátorem buňky CI (Cell Identifier), který má maximálně 2 x 8 bitů. Aby bylo možné od sebe odlišit sousední BTS, používá se identifikační kód základnových stanic BSIC (Base Transceiver Station Identity Code), který se skládá ze dvou částí:

- *kód mobilní sítě NCC (Network Color Code)*, 3 bity;
- *kód základnové stanice BCC (Base Transceiver Station Color Code)*, 3 bity;

BSIC je pravidelně vysílán základnovou stanicí. Přímo sousedící mobilní sítě musí mít různá NCC, stejně jako sousedící BTS musí mít rozdílná BCC [2].

3.3 Autentizace

Úkolem autentizace je zabezpečení ověření karty SIM, která žádá o přístup do sítě. Ověřování probíhá metodou výzev a odpovědí za účasti autentizačního klíče K_i každého uživatele, který je spolu s algoritmem A3 uložen na kartě SIM a na straně sítě v autentizačním centru AuC.

3.4 Šifrování dat

Zabezpečení dat přenášených přes rádiové rozhraní je realizováno použitím šifrování, kde jsou sekvence bitů transformovány matematicko-logickými operacemi na jiné sekvence bitů. Počet transformací operací je dán šifrovacím klíčem K_c, který je počítán při procesu autentizace. Provádění šifrování se uskutečňuje pouze nad hovorovými, datovými signály účastníka a některými signalizačními signály. Šifruje se tedy jen 114 bitů burstu, ostatní bity šifrovány nejsou.

4 Zpracování signálu v systému GSM

4.1 Způsoby přenosu

V komunikaci obecně rozlišujeme způsoby přenosu dle toho, jakým směrem probíhá komunikace mezi dvěma stranami. Simplexní přenos znamená komunikaci pouze jedním směrem. U GSM se simpexní přenos používá například pro distribuci informací k účastníkům (paging). Poloduplexní přenos umožňuje komunikaci oběma směry. Ovšem vysílání a příjem informací neprobíhá současně, mezi oběma fázemi přenosu se přepíná při použití jednoho komunikačního kanálu. Plně obousměrný přenos se nazývá full-duplexní. Komunikace zde umožňuje simultánní vysílání a příjem. Moderní digitální systémy jsou vždy schopny plného duplexu. Pro duplex se používají dvě základní procedury: FDD (Frequency Division Duplex), za použití různých frekvenčních pásem pro každý směr provozu a TDD (Time Division Duplex), který přepíná směr provozu v časové oblasti.

4.1.1 Frequency Division Duplex

Frekvenční duplex byl použit již v analogových mobilních rádiových systémech a je využíván v dnešních digitálních systémech. Pro komunikaci mezi mobilním zařízením a základnovou stanicí, je k dispozici kmitočtové pásmo rozdělené do dvou dílčích pásem pro současný příjem i vysílání. Jedno dílčí pásmo je vyhrazeno pro uplink (přenos z mobilního zařízení do základnové stanice) a další pásmo je vyhrazeno pro downlink (přenos od základnové stanice k mobilnímu zařízení). Pro dosažení dobré separace obou směrů musí mít dílčí pásma dostatečný odstup frekvencí. Obvykle se používá stejná anténa pro odesílání a příjem. Pro směrové oddělení je použita duplexní jednotka, skládající se v podstatě ze dvou úzkopásmových filtrů se strmými hranami.

4.1.2 Time Division Duplex

Tato technika umožňuje příjem a vysílání pouze kvazi-simultánně v různých časových úsecích, tj. směrové oddělení provozů probíhá přepínáním v čase mezi vysíláním a příjmem. Přepínání je velmi rychlé, komunikace se pak zdá být jako full-duplexní. Nicméně

z periodického intervalu T dostupného pro přenos z časového úseku může být použita pouze malá část, takže TDD vyžaduje dvakrát vyšší přenosové rychlosti než FDD.

4.2 Přístupové techniky

Komunikační médium je sdíleno mnoha uživateli, kteří mezi sebou soupeří o prostředky pro přenos svých datových proudů. Aby nedocházelo ke kolizím v přístupu k médiu mezi jednotlivými účastníky, je zapotřebí řídit jejich přístup přístupovým technikami. Tyto techniky mají za úlohu rozdělit přenosové médium na jednotlivé komunikační kanály. Využívají se techniky FDMA (Frequency Division Multiple Access), TDMA (Time Division Multiple Access) a CDMA (Code Division Multiple Access).

4.3 Kanály

Fyzická vrstva systému GSM sídlí na první ze sedmi vrstev RM - OSI (Reference Model - Open Systems Interconnection), obsahuje velmi složité funkce. Fyzické kanály jsou zde definovány prostřednictvím systému TDMA. Nad fyzickými kanály jsou definovány logické kanály, které jsou přenášeny v časových slotech fyzických kanálů. Logické kanály zastávají mnoho funkcí, jako přenos užitečných informací, signalizaci, vysílání obecných informací systému, synchronizaci a přidělení kanálů.

4.3.1 Logické kanály

Na první vrstvě OSI referenčního modelu, GSM definuje řadu logických kanálů, které jsou k dispozici buď v režimu nepřiděleném náhodného přístupu nebo ve vyhrazeném režimu určeném pro konkrétní uživatele. Logické kanály se dělí do dvou kategorií, provozní kanály a kanály signalizační (řídící).

4.3.1.1 Provozní kanály Provozní kanály TCH (Traffic Channels) se využívají pro přenos uživatelských dat (řeč, data). Komunikace přes tyto kanály muže být buď v režimu přepojování okruhů nebo přepojování paketů. V režimu přepojování okruhů poskytují provozní kanály transparentní datové připojení, které je speciálně upravené podle právě

poskytované služby (např. telefonování). Pro režim přepínání paketů nesou TCH uživatelská data druhé a třetí vrstvy OSI, dle doporučení X.25 normy nebo pakety podobných standardů protokolů. TCH mohou být kapacitně plně využity (full-rate TCH, TCH/F), nebo mohou být rozděleny na dva kanály s poloviční rychlostí (half-rate TCH, TCH/H), které můžou být poté rozděleny mezi různé účastníky. Dle ISDN terminologie se provozní kanály označují též jako Bm (mobilní B kanál) a Lm kanál (lower-rate mobilní kanál s poloviční přenosovou rychlostí). Pomocí Bm kanálu lze přenášet digitálně kódovanou řeč rychlostí 13 kbit/s, datové proudy rychlostí 14,5, 12, 6 nebo 3,6 kbit/s. Kanály Lm mají menší šířku pásma. Přenášejí hlasové signály s poloviční rychlostí (TCH/H) oproti Bm, nebo data rychlostmi 6 nebo 3,6 kbit/s [2].

4.3.1.2 Signalizační kanály

Řízení GSM sítě vyžaduje vysoké nároky na signalizaci, dokonce i když není vytvořeno aktivní spojení. Signalizační kanály zajišťují kontinuální paketově orientovanou signalizaci. Signalizační kanály můžeme rozdělit na vysílací kanál BCH (Broadcast Channel), běžný řídící kanál CCCH (Common Conttrol Channel) a dedikovaný řídící kanál DCCH (Dedicated Control Channel). Simplexní BCH kanály jsou využívány pro předání informací všem mobilním stanicím v příslušné buňce[3].

- *Řídící vysílací kanál BCCH (Broadcast Control Channel)* - tento kanál zprostředkovává informační prvky mobilním stanicím o organizaci sítě, jako jsou informace o konfiguraci rádiového kanálu aktuálně používané buňky a kanálech sousedních buněk, synchronizační informace, a registrační identifikátory LAI, CI, BSIC. V podstatě informace o organizační struktuře CCCH lokální BTS. BCCH je vysílán na prvním kmitočtu přiřazené buňky.

- *Frekvenčně korekční kanál FCCH (Frequency Correction Channel)* - FCCH předává informace mobilním stanicím o korekcích vysílacího kmitočtu.

- *Synchronizační kanál SCH (Synchronization Channel)* - vysílá informace o identitě BTS (např. BSIC) a data pro rámcovou synchronizaci.

FCCH a SCH jsou důležité pro provoz rádiového subsystému. Operují v rámci protokolu první vrstvy. Z druhé vrstvy k informacím těchto kanálů není přístup navzdory tomu, že údaje jsou zapotřebí ve třetí vrstvě pro správu rádiových zdrojů. Tyto dva kanály jsou vysílány společně s BCCH. CCCH je tzv. point-to-multipoint orientovaný signalizační kanál, pro řešení funkcí správy přístupu. To zahrnuje přiřazování specializovaných kanálů a paging pro lokalizaci MS. Skládá se z následujících kanálů:

- *Kanál náhodného přístupu RACH (Random Access Channel)* - je uplink část pro CCCH. Pomocí tohoto kanálu mobilní stanice zasílá požadavek síti o přístup, pokud chce zahájit přenos.
- *Potvrzovací kanál AGCH (Access Grant Channel)* - Kanál pro potvrzení nebo zamítnutí požadavku k přístupu MS k síti.
- *Kanál pro paging PCH (Paging Channel)* - je používán pro vyhledávání MS základnovou stanicí, která chce navázat s MS kontakt. MS jsou volány na základě TMSI nebo IMSI všemi BTS v aktuální LA. Pokud MS neodpoví v určeném časovém intervalu, jsou považovány za nedostupné.
- *Oznamovací kanál NCH (Notification Channel)* - slouží k informování MS o příchozích hovorech.

Posledním typem signalizačního kanálu je duplexní point-to-point orientovaný kanál DCCH.

- *Samostatný přidělený řídící kanál SDCCH (Standalone Dedicated Control CHannel)* - slouží pro komunikaci mezi MS a BTS před přidělením provozního kanálu nebo k přenosu krátkých textových zpráv. Je použit v situacích kdy není přidělen TCH, ke kterému by bylo možné asociovat FACCH nebo SACCH.
- *Pomalý přidružený řídící kanál SACCH (Slow Associated Control Channel)* - jakmile je aktivní provozní kanál použije se SACCH k přenosu informací synchronizace.

- *Rychlý přidružený řídící kanál FACCH (Fast Associated Control Channel)* - používá se při nedostatku rychlosti kanálu SACCH, použitím poloviny nebo celého burstu SACCH, pro řízení existujícího spojení.

Kromě těchto kanálů je definován *vysílací kanál buňky CBCH (Cell Broadcast Channel)*, pro vysílání zpráv služby krátkých textových zpráv buňky SMSCB (Short Message Service Cell Broadcast).CBCH sdílí fyzický kanál s SDCCH.

Skupina	**Typ**	**Značka**	**Kanál**	**Směr provozu**
Společný přístup	BCH Rozhlasové kanály	FCCH	Korekce kmitočtu	Downlink
		SCH	Synchronizace	Downlink
		BCCH	Řídící vysílací	Downlink
	CCCH Kanály všeobecného řízení	PCH	Pagingu	Downlink
		RACH	Náhodného přístupu	Uplink
		AGCH	Potvrzení přístupu	Downlink
		NCH	Oznamovací	Downlink
		CBCH	Buňkový vysílací	Downlink
Uživatelsky specifické řídící kanály	DCCH Vyhrazené řídící kanály	SDCCH	Samostatný přidělený	Duplexní
		SACCH	Pomalý přidružený	Duplexní
		FACCH	Rychlý přidružený	Duplexní

Tabulka 4.1: Přehled signalizačních kanálů

4.3.2 Fyzické kanály

Fyzické kanály přepravují logické kanály přes bezdrátové rozhraní. Fyzický kanál je definován jako určitý časový úsek na určitém kmitočtovém kanále.

4.4 Výkonové úrovně

V systému GSM se dělí do výkonových tříd BTS a MS, podle maximálního možného vysílacího výkonu. Tyto třídy jsou zobrazeny v tabulce 4.2 spolu s maximálním výkonem stanice v dané třídě.

Výkonová třída	Maximální výkon MS	Maximální výkon BTS
1	20 W (43 dBm)	320 W (55 dBm)
2	8W (39 dBm)	160 W (52 dBm
3	5 W (37 dBm)	80 W (49 dBm)
4	2 W (33 dBm)	40 W (46 dBm)
5	0,5 W (29 dBm)	20 W (43 dBm)
6	-	10 W (40 dBm)
7	-	5 W (37 dBm)
8	-	2,5 W (34 dBm)

Tabulka 4.2: Výkonové úrovně MS a BTS v systému GSM

Pro úsporu energie a limitaci interferencí se výkony stanic dynamicky mění. Úrovně výkonů jsou nastavovány na hodnoty, které postačí pro udržení kvality spojení, jejímž kritériem je bitová chybovost BER (Bit Error Ratio). Minimálním výkonem mobilní stanice je 20 mW tj. 13 dBm.

Menšími výkony disponují BTS určené pro pikobuňky a mikrobuňky pro GSM - Phase 2 a dělí se do tříd M1, M2 a M3. Třída M1 má maximální výkon 0,25 W (24 dBm), třída M2 má 0,08 W (19 dBm) a třída M3 může disponovat maximálním výkonem 0,03 W (14 dBm).

4.5 Handover

Přepnutí aktivního spojení mezi MS a BTS z jednoho rádiového kanálu na jiný kanál se nazývá handover. Důvod k přepnutí může mít rádiovou nebo síťovou příčinu, pokud systém vyhodnotí nový kanál jako kvalitnější. Může k němu vést rušení stávají-

cího kanálu, přechod do oblasti pokryté jinou buňkou, veliké zpoždění signálu nebo při rozložení zátěže sítě kvůli optimalizaci vytížení apod. Přepojení probíhá v krátkém čase automaticky, bez nutnosti zásahu uživatele MS, který přepojení nikterak nepostřehne. V systému je vyžadována informace o vždy aktuálním umístění MS, alespoň na úrovni buněk. Přepojení může mít různé průběhy, dle kterých se rozlišuje na tvrdý, bezešvý a měkký handover [4].

- *Tvrdý handover* - Systém odpojí MS od aktuálně užívaného kanálu a poté ji připojí na kanál nový. U tohoto přepojení vzniká krátké přerušení spojení do 100 ms. Toto přerušení je u přenosu hovorového signálu nepostřehnutelné, avšak u datového spojení přepojení může způsobit ztrátu informace. Synchronizací základových stanic lze dosáhnout snížení doby přepojení.

- *Bezešvý handover* - Před samotným přepojením je vytvořeno paralelně spojení na novém kanále a teprve po přepojení je spojení na původním kanále rozpojeno.

- *Měkký handover* - Mobilní stanice je neustále připojena k minimálně dvěma dostupným základnovým stanicím. Komunikace pak probíhá na všech kanálech. Během pohybu MS v síti jsou některá spojení rušena a jiné nově navazována. Tato technika klade vysoké nároky na kapacitu sítě.

Dále lze handover rozdělit podle toho, jaká část systému provádí měření kvality spojení, dle čehož rozhoduje o handoveru a řídí jej.

- *Sítí řízený handover NCHO (Network Controlled Handover)* - Mobilní stanice vysílá kontrolní signál, na základě jeho přijetí a zpracování výsledků systémem příslušné základnové stanice, se provádí rozhodnutí o případném přepnutí. To klade minimální požadavky na mobilní stanici, avšak tato metoda klade vyšší nároky na kapacitu tras mezi jednotlivými BTS radiotelefonní ústřednou.

- *Handover řízený mobilní stanicí MCHO (Mobile Controlled Handover)* - Měření kvality všech kanálů zajišťuje jak mobilní, tak i základnová stanice. Rozhodovací proces provádí MS a o jeho výsledku informuje systém, který zajistí přepnutí.

- *Sítí řízený handover s asistencí mobilní stanice MAHO (Mobile Assisted Handover)* - MS průběžně monitoruje výkonové hladiny signálů sousedních BTS a výsledky předává servisní základnové stanici. Měření aktuálního spojení realizuje MS i BTS současně. Systém na základě těchto poskytovaných informací uskutečňuje rozhodnutí o přepnutí spojení, jež následně provede.

Z hlediska buňkové struktury lze rozlišovat zda handover probíhá v rámci jedné buňky tzv. vnitřní handover, nebo mezi dvěma sousedními buňkami, kde se pak jedná o mezibuňkový handover.

- *Vnitřní handover* - Zde probíhá přelaďování mobilní stanice při pohybu uvnitř jedné buňky. Je to zapříčiněno tím, že během komunikace se mohou vyskytnout kanály (v rámci jedné buňky), které mohou poskytnout lepší parametry pro spojení, než kanál na kterém probíhá aktuálně komunikace.
- *Mezibuňkový handover* - Přepojování MS probíhá při jejich přechodu mezi buňkami.

5 Specifikace požadavků

5.1 Obecný popis

Aplikace bude primárně zaměřena pro servisní techniky GSM systému, pro sledování identifikátorů sítě. Dále bude umožňovat zapisování parametrů do souboru, pro pozdější analýzu. Aplikace bude mít přehledné uživatelské rozhraní v českém jazyce, které se dále bude skládat z několika obrazovek, na kterých bude vždy určitá skupina parametrů týkající se GSM, E/GPRS na samostatné obrazovce. Preferovaným formátem zobrazovaných parametrů je dekadický a v případě úrovní dB mód. Konfigurace bude umožňovat nastavení intervalu aktualizace identifikátorů a možnost volby povolení nebo zakázání zapisování logování. Nastavení logování bude mít možnost zapisovat data v časovém intervalu aktualizace parametrů, nebo při změně servisní buňky. Zapisovány budou všechny parametry spolu s časovou značkou. Aplikace bude mít možnost, dle získaných údajů, vyhledat v databázi geografické umístění servisní buňky a popis polohy zobrazit. Geografické umístění buňky bude také ukládáno spolu s ostatními identifikátory do logovacího souboru.

5.2 Hardwarové požadavky

Hardwarové požadavky vznikly na základě převahy přístrojů společnosti HTC na českém trhu. Požadavek na mobilní zařízení je tedy využití zařízení s integrovaným modulem GSM, například HTC Touch, HTC Blue Angel, HTC Magician, HTC Touch Diamond atd.

5.3 Softwarové požadavky

Z hardwarových požadavků vyplývá požadavek na operační systém Windows Mobile ve verzích 5.0, 6.0, 6.1. Finální aplikace bude pracovat nad platformou .NET společnosti Microsoft, konkrétně tedy .NET Compact Framework aktuální verze. Výběr vývojového prostředí je ponechán na volbě řešitele, stejně tak výběr programovacího jazyka.

6 Použité metodiky a technologie

6.1 Použité metodiky

6.1.1 UML

UML (Unified Modeling Language) je grafický jazyk pro objektově orientovanou analýzu a návrh softwaru, sloužící k popisu architektury vyvíjeného softwaru z hledisek důležitých pro analýzu a návrh. Jazyk využívá grafické konstruktory, nazývané diagramy.

6.2 Použité technologie

6.2.1 Operační systém Windows Mobile

Operační systém Windows Mobile od společnosti Microsoft, vychází z platformy Windows CE. Primárně je určen pro mobilní zařízení MDA (Mobile Device Assistent) a Smartphone. První verze systému byly označovány jako Pocket PC 2000, 2002 a 2003. Verze systému WM od 6.0 a výše jsou založeny na Windows CE 5.2. Dnes nejnovější verzí tohoto systému je verze Windows Mobile 6.5.5, avšak Microsoft chystá novou verzi s názvem Windows Mobile 7. Instalovaný systém v zařízení musí být optimalizován pro daný typ procesoru v zařízení, např. pro procesory ARM (Advanced RISC Machine), MIPS (Microprocessor without Interlocked Pipeline Stages) atp. Výsledná aplikace byla vyvíjena na zařízeních s OS Windows Mobile verze 5.0 a 6.1.

6.2.2 Platforma .NET Compact Framework

Microsoft .NET CF je navržen pro systémy Windows Mobile a Windows CE pro optimální výkon v rámci omezení zdrojů zařízení. .NET Compact Framework dědí v plné míře CLR (Common Language Runtime), dále podmnožinu .NET Framework Class Library, která podporuje funkce jako WCF (Windows Communication Foundation), a také Windows Forms. Též obsahuje třídy určené pouze pro .NET Compact Framework a řízené spouštění kódu. Platforma podporuje programovací jazyky *Visual Basic*, *C#*, *C++* a další. Framework použitý pří vývoji byl v nejaktuálnější verzi, tedy 3.5.

6.2.3 Jazyk C#

C# je objektově orientovaný jazyk, který byl vyvinut firmou Microsoft spolu s platformou .NET Framework. Je založen na jazycích *C++* a *Java*, které jsou založeny na jazyku *C*. Tento jazyk řeší (mimo jiné) problém složitostí mnohonásobných dědičností tím, že každá třída může být potomkem pouze jediné třídy. *C#* je používán se strukturou CLI (Common Language Infrastructure).

6.2.4 Microsoft Visual Studio 2008 Professional Edition

Grafické vývojové prostředí od Microsoftu, Visual Studio 2008 Professional Edition poskytuje vývojové nástroje, ladící funkce, funkce pro práci s databázemi pro vývoj aplikací různých druhů, pro několik platforem (Microsoft Windows, Windows CE, Windows Mobile, .NET, .NET Compact Framework a Microsoft Silverlight). Nedílnou součástí vývojových nástrojů jsou dokumentace, kde hlavním zdrojem pro implementaci mi bylo MSDN Libary a Windows Mobile 6 Professional SDK. Toto vývojové prostředí jsem vybral proto, že je velmi přátelské, co se týče vývoje pro mobilní zařízení a je poskytované VŠB-TU pod licencí Microsoft Developer Network Academic Alliance od firmy Microsoft.

6.2.5 Mobilní zařízení

Jako mobilní zařízení jsem zvolil MDA od společnosti HTC, konkrétně model P4500, též označovaný jako HTC TyTN (obrázek 6.1) nebo také Hermes, MDA Vario II apod. Zařízení se vyskytuje na trhu v několika provedení lišící se hlavně designem a drobnými odlišnosti v hardwaru. Konkrétní hardwarová specifikace je uvedena v tabulce 9.3. Zařízení je standardně vybaveno operačním systémem Windows Mobile verze 5.0. Vzhledem k tomu, že tato verze systému je poměrně staršího data vydání, aktualizoval jsem systém na verzi 6.1. Spolu se systémem jsem aktualizoval i verzi firmware, který obsluhuje GSM modem na aktuální verzi.

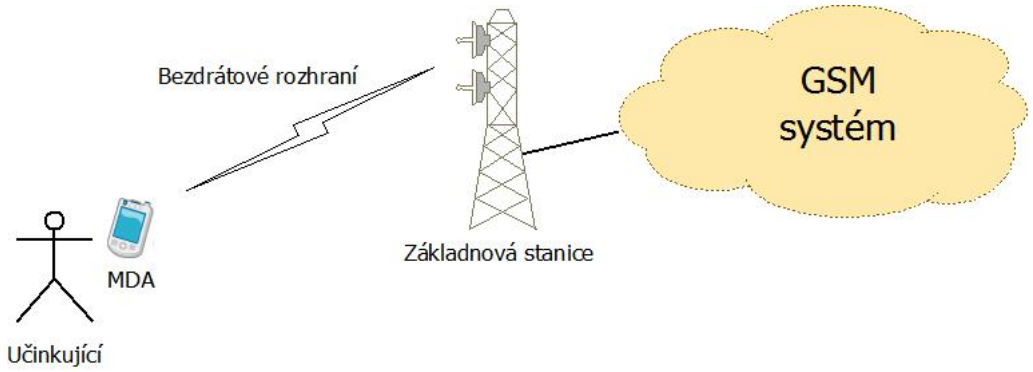
Obrázek 6.1: MDA HTC TyTN

HTC TyTN - specifikace	
procesor	Samsung SC32442AL-43S na frekvenci 400 MHz
displej	dotykový, QVGA (240 × 320 bodů), 65 tisíc barev
paměť	128Mb NAND Flash + 64Mb Mobile SDRAM
čipová sada	Qualcomm MSM6275
sítě	GSM 850/900/1 800/1 900 MHz a UMTS 2 100 MHz
data	GPRS, EDGE, UMTS, HSDPA, Wi-Fi, Bluetooth, IrDA
operační systém	Windows Mobile 6.1 Professional (Build 19199.0.7.0)
verze rádia	1.16.00

Tabulka 6.1: Specifikace zařízení HTC TyTN

7 Analýza a návrh

Základní analýzu zobrazuje blokový diagram na obrázku 7.1. V roli účinkujícího je předpokládán servisní technik, který pomocí MDA zjišťuje identifikátory sítě. Aplikace komunikuje s interním GSM modulem, který získává identifikátory z bezdrátového rozhraní od základnové stanice, která je součástí GSM systému.

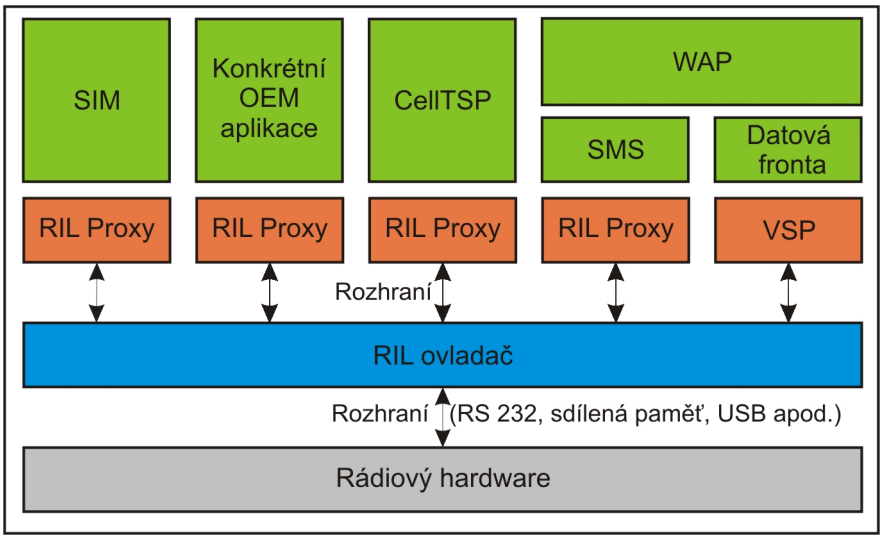


Obrázek 7.1: Blokový diagram analýzy

7.1 Analýza rozhraní MDA pro komunikaci s GSM modulem pro Windows Mobile

V systému Windows Mobile je implementovaná vrstva rádiového rozhraní RIL (Radio Interface Layer), speciálně vyvinutá pro tuto platformu. Tato vrstva poskytuje rozhraní pro komunikaci mezi systémovým softwarem CellCore a rádiovým hardwarem. RIL poskytuje abstraktní vrstvu umožňující vytvořit specifický ovladač, který může být implementován na různých rádiových hardwarech. RIL, bez ohledu na konkrétní detaily implementace, musí být podporován a v souladu s horními vrstvy systému jako TAPI (Telephony Application Programming Interface), ExTAPI (Extended API), SIM API apod. Vrstva zajišťuje služby na základě systémových požadavků pro komunikační funkce, např. hlas, data, službu krátkých textových zpráv. Zajišťuje také asynchronní notifikace na změny v systému, jako je změna úrovně signálu, příchozí požadavek na hovor, příchozí SMS zprávy. Telekomunikační služby ve Windows Mobile jsou definovány operačním

systémem. Funkce a služby by měly být v ideálním případě nezávislé na konkrétním rádiovém hardwaru. Architektura RIL je definovaná tak, že Windows Mobile poskytuje standardní API na principu mechanizmů požadavků a odpovědí, které lze využít na různých platformách, kde konkrétní detaily operací jsou skryty před zbývající částí systému. Architektura RIL pro Windows Mobile je zobrazena na obrázku 7.2.



Obrázek 7.2: Architektura RIL pro Windows Mobile

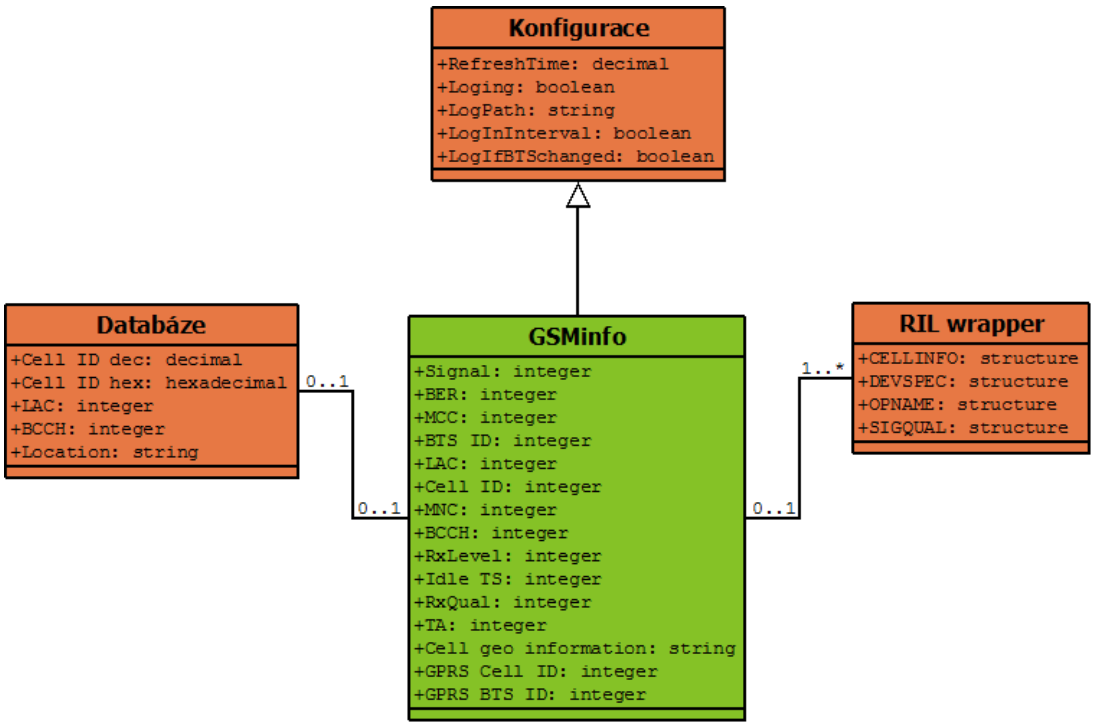
RIL komunikuje s GSM modulem pomocí AT příkazů. RIL funkce mohou být buď asynchronní nebo synchronní. Většina funkcí je asynchronní. Pro oba typy funkcí je vracen asynchronní výsledek funkce *HRESULT*, informující o úspěchu volání funkce. Pro asynchronní funkce pozitivní hodnoty *HRESULT* znamenají úspěšné volání funkce a používají se jako identifikátor příkazů pro odpovídající asynchronní volání. Asynchronní odpověď volání je vracena do vyrovnávací paměti. Záporné hodnoty *HRESULT* značí, že nastala chyba. Pro synchronní funkce se vrací hodnota S_OK znamenající úspěšné volání. Pokud synchronní funkce vrací užitečná data, je na ně odkazováno ukazatelem a data se ukládají do datových struktur [8].

Jak již vyplývá z definice vrstvy, výrobci konkrétních hardwarových řešení přizpůsobují ovladač RIL pro svá zařízení. To v praxi znamená, že některé funkce vrstvy nemusí být ovladačem a tedy i hardwarem podporované. Naopak v případě, že výrobce zahrne do

svého řešení rozšiřující funkce, je možné k nim přistupovat pomocí univerzálního přístupového bodu vrstvy, v podobě funkce implementované ve vrstvě. Konkrétní funkce se nazývá *„RIL_DevSpecific“*. Samotný název vypovídá o tom, že se jedná o funkci, která je tzv. *„Device Specific“*, tedy specifická pro konkrétní zařízení.

7.2 Konceptuální datový model

Konceptuální datový model, který zobrazuje diagram tříd (obrázek 7.3), ilustruje základní entity a vztahy nezbytné pro realizaci monitorování parametrů GSM 2. generace.



Obrázek 7.3: Diagram tříd - konceptuální datový model

GSMinfo - základní entita

Konfigurace - entita, od které jsou odvozeny vlastnosti základní entity

Databáze - entita obsahující položky informací o buňkách

RIL wrapper - entita zprostředkovávající komunikaci s GSM modemem

7.2.1 Seznam a popis atributů

V následujících tabulkách (7.1 až 7.4) jsou uvedeny všechny atributy všech entit konceptu.

Entita Konfigurace		
Název Atributu	**Datový typ**	**Význam atributu**
RefreshTime	int	časový údaj aktualizace parametrů
Loging	bool	reprezentuje stav povolení logování
LogPath	string	udává cestu k souboru logování
LogInInterval	bool	reprezentuje možný způsob logování
LogIfBTSchanged	bool	reprezentuje možný způsob logování

Tabulka 7.1: Seznam a popis atributů entity Konfigurace

Entita Databáze		
Název Atributu	**Datový typ**	**Význam atributu**
Cell ID dec	dec	identifikační číslo buňky v dec. tvaru
Cell ID hex	hex	identifikační číslo buňky v hex. tvaru
LAC	int	Local Area Code - kód oblasti
BCCH	int	Broadcast Control Chanel - vysílací řídící kanál
Location	string	Informace o geografickém umístění buňky

Tabulka 7.2: Seznam a popis atributů entity Databáze

Entita GSMinfo

Název Atributu	Datový typ	Význam atributu
Signal	int	úroveň signálu
BER	int	Bit Error Rate - bitová chybovost udávaná v
MCC	int	Mobile Country Code - kód země
BTS	int	Base Transcieve ID - kód základnové stanice
LAC	int	Location Area Code - kód oblasti
Cell ID	int	identifikační číslo buňky
MNC	int	Mobile Network Code - kód sítě
BCCH	int	Broadcast Control Chanel - vysílací řídící kanál
RxLevel	int	úroveň přijímaného signálu
Idle TS	int	Idele Time Slot - časový slot
RxQual	int	kvalita přijímaného signálu
TA	int	Timing Advance
Cell geo information	string	informace o geografickém umístění buňky
GPRS Cell ID	int	identifikační číslo GPRS buňky
GPRS BTS ID	int	identifikační číslo základnové stanice BPRS

Tabulka 7.3: Seznam a popis atributů entity GSMinfo

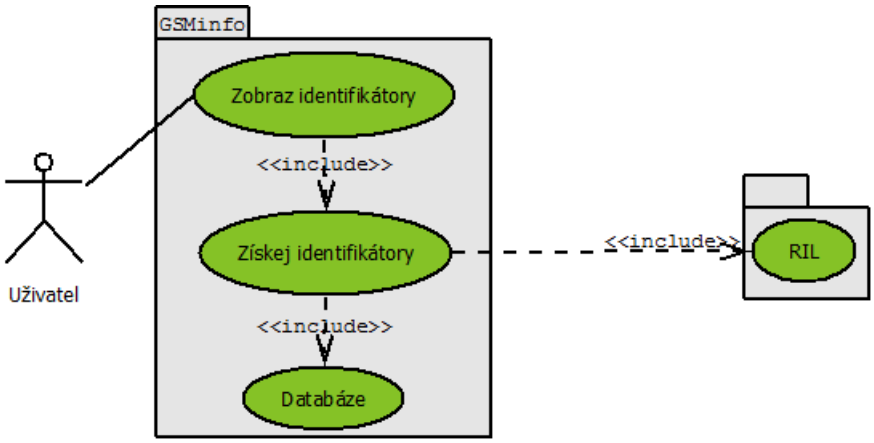
Entita RIL wrapper

Název Atributu	Datový typ	Význam atributu
CELLINFO	struct	struktura obsahující identifikátory buňky
DEVSPEC	struct	struktura univerzálního přístupového bodu
OPNAME	struct	struktura jmen operátora
SIGQUAL	struct	struktura informací signálu

Tabulka 7.4: Seznam a popis atributů entity RIL wrapper

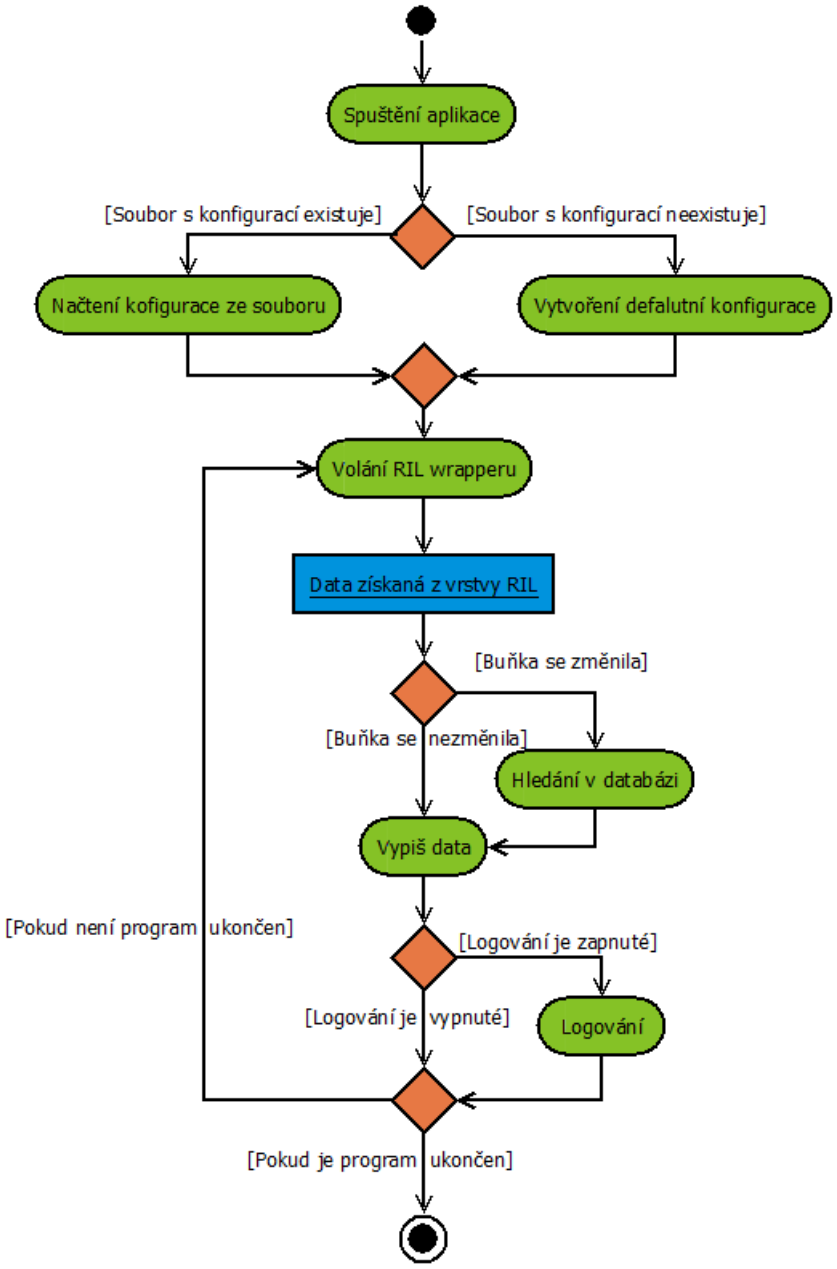
7.3 Analýza případu užití

Případ užití zobrazuje use case diagram na obrázku 7.4. Uživatel zažádá spuštěním aplikace o zobrazení identifikátorů, které se následně zobrazí pomocí GUI (Graphic User Interface). Zjednodušený proces ilustruje diagram aktivit.



Obrázek 7.4: Use case - požadavek na zobrazení identifikátorů

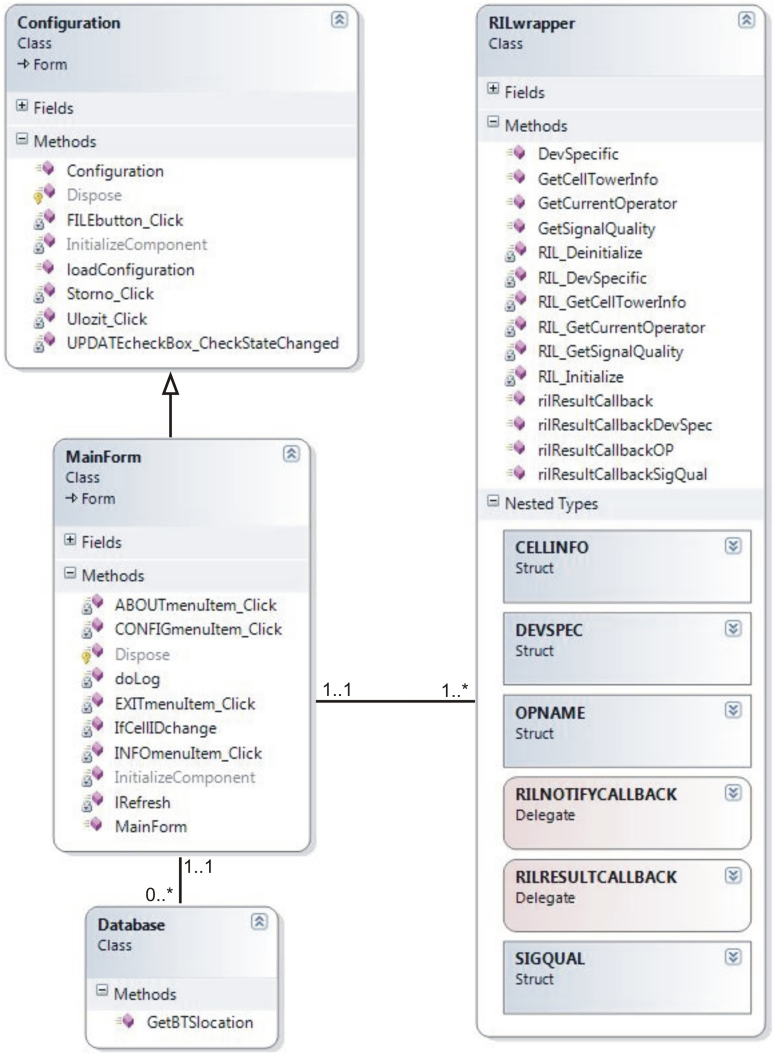
Diagram aktivit na obrázku 7.5 znázorňuje počáteční inicializaci a následný běh aplikace. Nejprve je zkontrolována přítomnost konfiguračního souboru pro nastavení aplikace. Druhým krokem je zavolání RIL wrapperu, který získává pomocí vrstvy RIL potřebná data, které následně zobrazí obsluze zařízení a případně provede zápis parametrů do souboru. Proces volání RIL wrapperu, zobrazování parametrů a případný zápis do souboru se opakuje v zadaném intervalu až do ukončení aplikace.



Obrázek 7.5: Diagram aktivit GSMinfo

8 Implementace

Implementace navržených algoritmů probíhala na základě zvolené technologie .NET, pomocí standardních knihoven a knihovny *ril.dll*. Třídní diagram na obrázku 8.1 zobrazuje vazby mezi třídy a jejich metody. Popis jednotlivých tříd a jejich metod je součástí programové dokumentace v příloze č.II.



Obrázek 8.1: Diagram tříd GSMinfo

8.1 Přístup k informacím vrstvy RIL

Pro získání informací z rádiového rozhraní je zapotřebí uvnitř vlastní aplikace vytvořit spojení s vrstvou rádiového rozhraní. RIL publikuje několik API, všechny označené s prefixem „RIL_“. Všechna API vrstvy jsou napsány v nativním kódu. To znamená, že pro jejich použití v řízených aplikacích je nutné použít P / Invoke. Přístup k API vrstvy RIL z řízeného kódu pomocí P / Invoke, ukazuje následující mnou použitý případ:

```
public delegate void RILRESULTCALLBACK(uint dwCode, IntPtr hrCmdID, IntPtr lbData, uint
    cbData, uint dwParam);
public delegate void RILNOTIFYCALLBACK(uint dwCode, IntPtr lbData, uint cbData, uint
    dwParam);


    [DllImport("ril.dll")]
    private static extern IntPtr  RIL_Initialize (uint dwIndex,RILRESULTCALLBACK
        pfnResult,RILNOTIFYCALLBACK pfnNotify,uint dwNotificationClasses, uint dwParam,
        out IntPtr lphRil);
    [DllImport("ril.dll")]
    private static extern IntPtr RIL_GetCellTowerInfo(IntPtr hRil);
    [DllImport("ril.dll")]
    private static extern IntPtr RIL_GetSignalQuality(IntPtr hRil);
    [DllImport("ril.dll")]
    private static extern IntPtr RIL_DevSpecific(IntPtr hRil, IntPtr lbData, int dwSize);
    [DllImport("ril.dll")]
    private static extern IntPtr RIL_GetCurrentOperator(IntPtr hRil, uint dwFormat);
    [DllImport("ril.dll")]
    private static extern IntPtr  RIL_Deinitialize ( IntPtr  hRil);
```

Výpis 1: Ukázka přístupu k API vrstvy RIL

Pro získání požadovaných informací od rádiové vrstvy se volá příslušná funkce RIL. Nicméně je zapotřebí volat další funkce pro obsluhu, tedy pro inicializaci a po provedení požadovaných funkcí následnou deinicializaci vrstvy, která uvolní a uzavře použité zdroje.

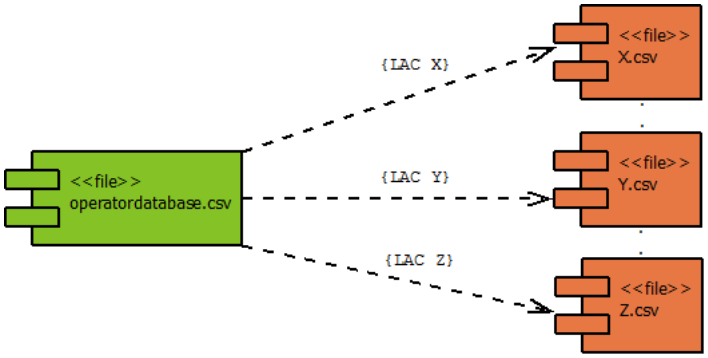
8.1.1 Implementace pomocí vláken

Inicializační funkce vrstvy vytváří *handle* pro specifické funkce. Pro každou aplikaci v systému požadující přístup k vrstvě RIL je načtena RIL Proxy, která udržuje unikátní *handles* klientů (role klienta se zde rozumí aplikace nebo systém). RIL Proxy řídí přístup k vrstvě RIL. Aby nedošlo ke kolizi v požadavcích na přístup k vrstvě, řadí RIL Proxy požadavky do front [9]. Jelikož k vrstvě RIL může přistupovat několik aplikací i systém současně, může být odezva na volanou funkci dlouhá (v důsledku dlouhé fronty), což by zapříčinilo čekání („zamrznutí“) aplikace. Tento problém jsem při implementaci vyřešil vytvořením nového vlákna, které obsluhuje zpětné volání vrstvy. Po inicializaci přístupu k vrstvě a následném zavolání specifické funkce se vytváří nové vlákno, čekající na výsledek volání specifické funkce. Po obdržení výsledků od vrstvy RIL zpracuje vlákno pro obsluhu data vrstvy a předá je hlavnímu vláknu, kde jsou data dále zpracována a vlákno pro obsluhu zpětného volání vrstvy se automaticky uzavře.

8.2 Vyhledávání v databázi

Zařízení s operačním systémem Windows Mobile mají omezené zdroje (poměrně malou paměť pro aplikace, relativně pomalé procesory, pomalý souborový systém). Při implementaci na tyto omezení byl brán ohled. Databáze geografických umístění buněk jsou značně obsáhlé a to i přes to, že v řešení jsou zpracovávány databáze buněk systému GSM 2. generace s výskytem pouze na českém území a třech nejrozvinutějších operátorů. Průměrný počet záznamů v databázi jednoho operátora se pohybuje kolem dvanácti tisíc. Vyhledávání v takovéto neindexované databázi by znamenalo pro zařízení velké a relativně časově dlouhé zatížení. Pro optimalizaci výkonu vyhledávání jsem vytvořil aplikaci pro operační systém Windows a platformu .NET, která rozdělí obsáhlé databázové soubory na několik menších. Třídění probíhá na základě kódů oblasti z databáze operátora. Buňky náležící do jedné stejné oblasti jsou z původní databáze vyjmuty a zkopírovány do samostatného souboru. Proces třídění je zobrazen na obrázku 8.2. K informacím o buňce se tedy přistupuje na základě kódu oblasti a čísla buňky. Použití této aplikace je popsáno v uživatelském manuálu.

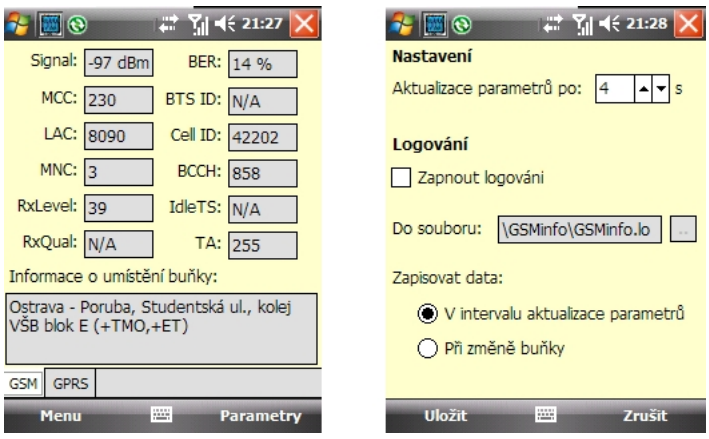
Toto řešení rapidně snížilo proces hledání v databázi, za symbolickou cenu delší instalace hlavní aplikace do zařízení. Použití aplikace je nutné pouze při prvotní instalaci databáze nebo při její aktualizaci. Databáze obsahující geografické umístění buněk operátorů na území ČR jsem získal z webu *http://gsmweb.cz/*, odkud je možné stáhnout aktualizované verze.



Obrázek 8.2: Princip třídění databáze buňek

8.3 Implementace GUI

Vytváření uživatelského prostředí probíhalo podle požadavků specifikace. Návrh probíhal použitím standardních grafických komponent použitím Microsoft Visual Studio 2008 Professional.



Obrázek 8.3: Implementace GUI

9 Testování aplikace v reálných podmínkách

Testování aplikace bylo prováděno na přístrojích převážně výrobce HTC s rozdílnými čipovými sadami a s operačním systémem ve verzích 5.0, 6.1 a 6.5. Pro porovnání jsem zařadil do testovacího plánu i zařízení jiných výrobců. Všechna testovaná zařízení měla nainstalována nejnovější .NET Copmpact Framework 3.5. Následující tabulkové zobrazení, vyjadřují podporu získání jednotlivých identifikátorů na konkrétních zařízení.

	Podpora zařízení			
Identifikátor	**HTC TyTN**	**HTC ELF**	**HTC HD 2**	**HTC PRO 2**
Signal	ANO	ANO	ANO	ANO
BER	NE	NE	NE	NE
MCC	ANO	NE	ANO	ANO
MNC	ANO	NE	ANO	ANO
LAC	ANO	ANO	ANO	ANO
Cell ID	ANO	ANO	ANO	ANO
BTS	NE	NE	NE	NE
BCCH	ANO	ANO	ANO	ANO
RxLevel	NE	NE	NE	NE
RxQual	NE	NE	NE	NE
Idle TS	NE	NE	NE	NE
TA	NE	NE	NE	NE
GPRS Cell ID	NE	NE	NE	NE
GPRS BTS ID	NE	NE	NE	NE

Tabulka 9.1: Podpora zařízení pro zobrazení identifikátorů

Z tabulek zobrazujících podporu zobrazení je vidět, jaké funkce implementoval výrobce do svého zařízení, konkrétně do ovladače GSM modulu, který se samozřejmě odvíjí od použitého hardwaru. Ovšem jak jsem se přesvědčil při testování, ne všichni výrobci píší ovladače pro svá zařízení tak, aby byly zpřístupněny všechny funkce GSM modemu

Identifikátor	Podpora zařízení		
	HTC DIAMOND II	**HTC VARIO**	**HTC TOUCH HD**
Signal	ANO	ANO	ANO
BER	NE	NE	NE
hline MCC	ANO	NE	ANO
MNC	ANO	NE	ANO
LAC	ANO	ANO	ANO
Cell ID	ANO	ANO	ANO
BTS	NE	NE	ANO
BCCH	ANO	ANO	ANO
RxLevel	NE	NE	ANO
RxQual	NE	NE	NE
Idle TS	NE	NE	NE
TA	NE	NE	NE
GPRS Cell ID	NE	NE	NE
GPRS BTS ID	NE	NE	NE

Tabulka 9.2: Podpora zařízení pro zobrazení identifikátorů

aplikační vrstvě operačního systému pomocí standardních funkcí. Je to zřejmě proto, že výrobci nepočítají s využitím těchto funkcí z vyšších vrstev, ačkoliv např. zařízení Mio a701 a Samsung Omnia, jsou na tom s podporou standardních funkcí o něco lépe.

Identifikátor	Podpora zařízení		
	E-TEN X800	**MIO A701**	**SAMSUNG OMNIA**
Signal	ANO	ANO	ANO
BER	ANO	NE	ANO
MCC	NE	ANO	ANO
MNC	NE	ANO	ANO
LAC	ANO	ANO	ANO
Cell ID	ANO	ANO	ANO
BTS	NE	ANO	NE
BCCH	ANO	ANO	ANO
RxLevel	NE	ANO	ANO
RxQual	NE	NE	NE
Idle TS	NE	NE	NE
TA	NE	ANO	NE
GPRS Cell ID	NE	NE	NE
GPRS BTS ID	NE	NE	NE

Tabulka 9.3: Podpora zařízení pro zobrazení identifikátorů

10 Závěr

Tato práce přináší objasnění problematiky získávání „low level“ parametrů GSM sítě pomocí zařízení postavených na systému Windows Mobile. Praktickým výsledkem je univerzální aplikace pro získávání parametrů GSM 2. generace, nezávislá na konkrétním zařízení. Aplikace je omezená pouze ze strany výrobce a to konkrétně na jeho volbě implementace ovladače GSM modemu. Aplikace je připravena na rozšíření prostřednictvím univerzálního přístupového bodu vrstvy RIL. Pro toto rozšíření je připravena funkce *RIL_DevSpecific*, implementovaná v třídě *RILwrapper*. Tato funkce vyžaduje specifické parametry, známé pouze výrobci zařízení nebo výrobci použité čipové sady. Výrobci se ovšem k poskytnutí těchto informací staví negativně, kvůli ochraně svého „know how“.

Využití tzv. „chytrých“ telefonů s operačním systémem Windows Mobile ke sledování identifikátorů GSM 2. generace je velice zajímavá možnost z hlediska servisních techniků systému GSM, protože tyto zařízení jsou v dnešní době jakýmsi standardním vybavením. Pro získání základních identifikátorů není zapotřebí složitých a drahých analyzačních přístrojů a základní analýza tak může proběhnout prakticky kdykoliv je zapotřebí. Na druhou stranu tyto mobilní přístroje nejsou dostatečně otevřeny pro tento směr využití, zejména kvůli uzavřenosti konkrétních implementací řešení výrobců těchto zařízení, ať už se jedná o hardware, či software v podobě ovladače modemu.

Z pohledu běžných uživatelů vidím možné využití hlavně ve znalosti identifikátorů, podle kterých lze určit orientační polohu. Tyto informace by mohli být využity například pro automatické změny profilu vyzvánění, nebo automatické zasílání SMS zpráv, v závislosti na geografické poloze zařízení a tedy i uživatele. Pro zjišťování přesné pozice se sice využívá systém GPS (Global Position System), avšak pro jeho využití je zapotřebí GPS modulu, kterým nejsou vybavena všechna zařízení, a dalším nedostatkem je velká energetická náročnost těchto modulů.

11 Reference

[1] HEINE, Gunnar; HORRER, Matt. *Gsm Networks.* : Artech House, Incorporated, 1998. 432 s.

[2] EBERSPÄCHER, Jörg, et al. GSM : *Architecture, Protocols and Services. 3rd edition. Great Britain : JohnWiley & SonsLtd, 2009. 317 s. ISBN 978-0-470-03070-7.*

[3] MOULY, Michel; PAUTET, Marie-Bernadette. *The GSM System for Mobile Communications.* : Telecom Publishing, 1992. 701 s.

[4] *Global System for Mobile Communications*. WILEY [online]. [cit. 2010-02-29]. Dostupný z WWW: <http://media.wiley.com/product_data/excerpt/64/04708233/0470823364.pdf>.

[5] STUBER, Gordon L., et al. *Principles Of Mobile Communication*. New York : Springer-Verlag New York, LLC, 2001. 780 s.

[6] MEHROTRA, Asha K. ; MEHROTRA, A. . *Gsm System Engineering.* [s.l.] : Artech House, Incorporated, 1997. 472 s.

[7] VONDRÁK, Ivo.*Úvod do softwarového inženýrství : verze 1.1*.Ostrava, 2002. 74 s. Scriptum. VŠB – Technická univerzita Ostrava, Fakulta elektrotechniky a informatiky, katedra informatiky.

[8] *Radio Interface Layer (RIL) White Paper*. [s.l.] : Microsoft Corporation, 2004. 44 s.

[9] Microsoft Corporation. *Microsoft Developer Network : MSDN Library*[online]. 2010 [cit. 2010-03-21]. Dostupné z WWW: <http://msdn.microsoft.com>.

[10] ECMA-334. *C# Language Specification. Geneva* : ECMA International, 2006. 508 s.

A Seznam příloh

I. Uživatelská dokumentace (obsažena na přiloženém CD-ROM)

II. Programátorská dokumentace (obsažena na přiloženém CD-ROM)

III. Přiložený CD-ROM